UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/530,574	04/07/2005	Masakatu Morii	Q87353	8988

23373 7590 09/12/2008

SUGHRUE MION, PLLC
2100 PENNSYLVANIA AVENUE, N.W.
SUITE 800
WASHINGTON, DC 20037

EXAMINER	
PACHURA, REBECCA L	
ART UNIT	**PAPER NUMBER**
2136	

MAIL DATE	DELIVERY MODE
09/12/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/530,574	MORII ET AL.	
	Examiner	Art Unit	
	Rebecca L. Pachura	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *07 April 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *07 April 2005* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☒ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *04/07/2005*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. **Claims 1-20 are presented for examination.**

The claims and only the claims form the metes and bounds of the invention. "Office personnel are to give claims their broadest reasonable interpretation in light of the supporting disclosure. In re Morris, 127 F.3d 1048, 1054-55, 44 USPQ2d 1023, 1027-28 (Fed. Cir. 1997). Limitations appearing in the specification but not recited in the claim are not read into the claim. In re Prater, 415 F.2d 1393, 1404-05, 162 USPQ 541, 550-551 (CCPA 1969)" (MPEP p 2100-8, c 2, I 45-48; p 2100-9, c 1, l 1-4). The Examiner has full latitude to interpret each claim in the broadest reasonable sense. The Examiner will reference prior art using terminology familiar to one of ordinary skill in the art. Such an approach is broad in concept and can be either explicit or implicit in meaning.

Information Disclosure Statement

2. The information disclosure statement filed 04/07/2005 fails to comply with the provisions of 37 CFR 1.97, 1.98 and MPEP § 609 because prior art # JP61246787 does not include an English translation abstract and one is not supplied at the esp@cenet database. It has been placed in the application file, but the information referred to therein has not been considered as to the merits. Applicant is advised that the date of any re-submission of any item of information contained in this information disclosure statement or the submission of any missing element(s) will be the date of submission for purposes of determining compliance with the requirements based on the time of filing the statement, including all certification requirements for statements under 37 CFR 1.97(e). See MPEP § 609.05(a).

Preliminary Amendment

3. The preliminary amendments to the claims and specification submitted on 04/07/2005 is duly noted.

Request for Corrected Official Filing Receipt

4. The request to change the title of the application from "Pseudo-Random Number Generation Method and Pseudo-Random Number Generator" to "Method for Generating Pseudo-Random Numbers and Pseudo-Random Number Generator" submitted on 10/27/2005 is duly noted.

Priority

5. The claim for foreign priority from # 2002-294184 from Japan filed on 10/07/2002 is duly noted.

Oath/Declaration

6. The oath or declaration is defective. A new oath or declaration in compliance with 37 CFR 1.67(a) identifying this application by application number and filing date is required. See MPEP §§ 602.01 and 602.02.

The oath or declaration is defective because: the priority date claimed is incorrect it states the priority date is 07/10/2002 instead of the correct date being 10/07/2002.

Specification

7. Applicant is reminded of the proper content of an abstract of the disclosure.

> A patent abstract is a concise statement of the technical disclosure of the patent and should include that which is new in the art to which the invention pertains. If the patent is of a basic nature, the entire technical disclosure may be new in the art, and the abstract should be directed to the entire disclosure. If the patent is in the nature of an improvement in an old apparatus, process, product, or composition, the abstract should include the technical disclosure of the improvement. In certain patents, particularly those for compounds and compositions, wherein the process for making and/or the use thereof are not obvious, the abstract should set forth a process for making and/or use thereof. If

the new technical disclosure involves modifications or alternatives, the abstract should mention by way of example the preferred modification or alternative.

The abstract should not refer to purported merits or speculative applications of the invention and should not compare the invention with the prior art.

Where applicable, the abstract should include the following:
(1) if a machine or apparatus, its organization and operation;
(2) if an article, its method of making;
(3) if a chemical compound, its identity and use;
(4) if a mixture, its ingredients;
(5) if a process, the steps.

Extensive mechanical and design details of apparatus should not be given.

Applicant is reminded of the proper language and format for an abstract of the disclosure.

The abstract should be in narrative form and generally limited to a single paragraph on a separate sheet within the range of 50 to 150 words. It is important that the abstract not exceed 150 words in length since the space provided for the abstract on the computer tape used by the printer is limited. The form and legal phraseology often used in patent claims, such as "means" and "said," should be avoided. The abstract should describe the disclosure sufficiently to assist readers in deciding whether there is a need for consulting the full patent text for details.

The language should be clear and concise and should not repeat information given in the title. It should avoid using phrases which can be implied, such as, "The disclosure concerns," "The disclosure defined by this invention," "The disclosure describes," etc.

The abstract of the disclosure is objected to because it does not make any sense it appears as if some words have been left out of the sentences. It also has an inappropriate number in the context. Correction is required. See MPEP § 608.01(b).

The disclosure is objected to because of the following informalities: Page 3, line 15 it states “in Fig. 14” it should state “in Fig. 18”. Appropriate correction is required.

The lengthy disclosure has not been checked to the extent necessary to determine the presence of all possible minor errors. Applicant's cooperation is requested in correcting any errors of which applicant may become aware in the specification. The examiner noticed many grammatical errors, missing words, and words in places that did not make any sense.

Drawings

8. The drawings were received on 04/07/2005. These drawings are not accepted.

Figures 16, 17, and 18 should be designated by a legend such as --Prior Art-- because only that which is old is illustrated. See MPEP § 608.02(g). Corrected drawings in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. The replacement sheet(s) should be labeled "Replacement Sheet" in the page header (as per 37 CFR 1.84(c)) so as not to obstruct any portion of the drawing figures. If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

The drawings are objected to under 37 CFR 1.83(a) because they fail to show "s" and "L" as described in the specification. Any structural detail that is essential for a proper understanding of the disclosed invention should be shown in the drawing. MPEP § 608.02(d). Corrected drawing sheets in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. The figure or figure number of an amended drawing should not be labeled as "amended." If a drawing figure is to be canceled, the appropriate figure must be removed from the replacement sheet, and where necessary, the remaining figures must be renumbered and appropriate changes made to the brief description of the several views of the drawings for consistency. Additional replacement sheets may be necessary to show the renumbering of the remaining figures. Each drawing sheet submitted after the filing date of an application must be labeled in the top margin as either "Replacement Sheet" or "New Sheet" pursuant to 37 CFR 1.121(d). If the changes are not accepted by the examiner, the applicant will be notified and

informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Claim Objections

9. Claims 2-20 are objected to because of the following informalities: Claims 2-4, 6, 8-13, and 15-20 state "A" line 1 first word when they should state "The"; claim 3, line 2 states "shift resistor" it should state "shift register"; claim 4, line 1 states "in any of claims 1" it should state "in claim 1"; claim 5, line 14 states "string every the number" not sure what it should state; claim 6, line 4 states "shift resistor" it should state "shift register"; claim 7, line 24 "means ever the number" not sure what it should state; claim 10, line 6 states "operation every the means" not sure what it should state; claim 13 is missing a lot of "the's, a's and 's" the examiner is not sure where because the claim does not even make sense; claim 14, line 25 states "means every the number" not sure what it should state; claim 16, line 8 states "to every each of" not sure what it should state; and claim 17, line 2 states "provided every each" not sure what it should state. Appropriate correction is required.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

10. **Claims 1, 2, 5, 7-10, 13, 14, 16, 17, and 19-20 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.**

The term "the above means" in claims 5, 7, 8, and 14 is a relative term which renders the claim indefinite. The term "the above means" is not defined by the claim, the specification does not provide a standard for ascertaining the requisite degree, and one of ordinary skill in the art would not be reasonably apprised of the scope of the invention.

Claim 1, 5, 7, and 14 recite the limitation "multiplying the bit number per one cycle by two or more to calculate" it is unclear to the examiner what the applicant is multiplying the bit number by two, three, five etc. or how this multiple is determined.

Claim 1 recites the limitation "the resistor" in line 15. There is insufficient antecedent basis for this limitation in the claim.

Claim 2 recites the limitation "the derived number" in line 3. There is insufficient antecedent basis for this limitation in the claim.

Claim 5 recites the limitation "the first linear feedback shift register" in line 11. There is insufficient antecedent basis for this limitation in the claim.

Claim 5 recites the limitation "the bit number" in 16. There is insufficient antecedent basis for this limitation in the claim.

Claim 5 recites the limitation "the number" in line 18. There is insufficient antecedent basis for this limitation in the claim.

Claim 5 recites the limitation "the resistor" in line 21. There is insufficient antecedent basis for this limitation in the claim.

Claim 7 recites the limitation "the number" in line 23. There is insufficient antecedent basis for this limitation in the claim.

Claim 7 recites the limitation "the resistor" in line 25. There is insufficient antecedent basis for this limitation in the claim.

Claim 7 recites the limitation "the means for outputting selectively used random number bit string" in line 34. There is insufficient antecedent basis for this limitation in the claim.

Claim 7 recites the limitation "the means for selecting the amplified random number bit string" in line 36. There is insufficient antecedent basis for this limitation in the claim.

Claim 9 recites the limitation "the means for outputting selectively used random number table" in lines 2, 5, 9, and 11. There is insufficient antecedent basis for this limitation in the claim.

Claim 9 recites the limitation "the means for generating" in line 7. There is insufficient antecedent basis for this limitation in the claim.

Claim 9 recites the limitation "the means for nonlinearly converting outputs pseudo-random numbers" in line 12. There is insufficient antecedent basis for this limitation in the claim.

Claim 9 recites the limitation "the means for generating the amplified random bit string" in line 14. There is insufficient antecedent basis for this limitation in the claim.

Claim 10 recites the limitation "the means for outputting selectively used random number bit string" in lines 2 and 6. There is insufficient antecedent basis for this limitation in the claim.

Claim 10 recites the limitation "the means for selecting the amplified random number bit string" in line 5. There is insufficient antecedent basis for this limitation in the claim.

Claim 13 recites the limitation "the same number" in line 3. There is insufficient antecedent basis for this limitation in the claim.

Claim 14 recites the limitation "the number" in line 25. There is insufficient antecedent basis for this limitation in the claim.

Claim 14 recites the limitation "the resistor" in line 27. There is insufficient antecedent basis for this limitation in the claim.

Claim 14 recites the limitation "the means for outputting selectively used random number bit string" in line 36. There is insufficient antecedent basis for this limitation in the claim.

Claim 14 recites the limitation "the means for selecting the amplified random number bit string" in line 38. There is insufficient antecedent basis for this limitation in the claim.

Claim 16 recites the limitation "the means for outputting selectively used random number table" in lines 2 and 4. There is insufficient antecedent basis for this limitation in the claim.

Claim 16 recites the limitation "the means for generating the amplified random bit string" in lines 6 and 13. There is insufficient antecedent basis for this limitation in the claim.

Claim 16 recites the limitation "the means for outputting selectively used random number bit string" in lines 8 and 10. There is insufficient antecedent basis for this limitation in the claim.

Claim 16 recites the limitation "the selectively used random number table" in line 9. There is insufficient antecedent basis for this limitation in the claim.

Claim 17 recites the limitation "the means for outputting selectively used random number bit string" in lines 2 and 6. There is insufficient antecedent basis for this limitation in the claim.

Claim 17 recites the limitation "the means for selecting the amplified random number bit string" in line 5. There is insufficient antecedent basis for this limitation in the claim.

Claim 19 recites the limitation "the means for outputting selectively used random number bit string" in line 3. There is insufficient antecedent basis for this limitation in the claim.

Claim 20 recites the limitation "the same number" in line 3. There is insufficient antecedent basis for this limitation in the claim.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

11. **Claims 1-20 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.** In the preamble of claims 1, 5, 7, 14, and 16 the applicant states that it is a method claim. In a method claim there must be a concrete, tangible, result associated with the method. The preamble recites *"for generating pseudo-random numbers"* this algorithm has no result in the limitations of the claim. In view of the below sited MPEP section the claim is non-statutory because it is nonfunctional descriptive material per se. Claims 14 and 16 recite *"A program to be executed by a computer"* a program is clearly software that must be embodied in something such as a storage device, a CD or a DVD, flash memory, etc. In view of the below sited MPEP section the claim is non-statutory because it is functional descriptive material per se.

As to the dependent claims 2-4, 6, 8-13, 15, and 17-20, are rejected as incorporating the deficiencies of the claims upon which they depend.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

12. **Claims 1-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over US 5600720 (Iwamura) in view of US 5434807 (Yoshida) and in view of US 20040076293 (Smeets).**

As to claim 1, Iwamura discloses a method for generating pseudo-random numbers comprising:

a first step for setting up an initial state value of a linear feedback shift register including n plurality of shift resistors and capable of outputting a bit string having bit number of (2 n)-1 per one cycle (Iwamura column 2, lines 42-52);

a third step for multiplying the derived value by a value obtained by multiplying the bit number per one cycle by two or more to calculate a bit number to be outputted from the linear feedback shift register (Iwamura column 3, lines 35-45);

a fourth step for outputting a bit string corresponding to the calculated bit number based on the initial state value from the linear feedback shift register (Iwamura column 9, lines 29-35);

a fifth step for taking out a bit from the output bit string to generate a new bit string (Iwamura column 9, lines 40-45);

a sixth step for reconstructing the linear feedback shift register such that the new bit string can be outputted from the resistor (Iwamura column 9, lines 19-55); and

a seventh step for generating pseudo-random numbers based on the initial state value from the reconstructed linear feedback shift register (Iwamura column 9, lines 19-55). Iwamura fails to teach a second step for finding a derived value prime to the bit number per one cycle of the linear feedback shift register based on the initial state value by means of a predetermined operation processing.

However, Yoshida discloses a second step for finding a derived value prime to the bit number per one cycle of the linear feedback shift register based on the initial state value by means of a predetermined operation processing (Yoshida column 1, lines 45-55);

It would be obvious to one of ordinary skill in the art at the time of the applicant's invention to combine Iwamura and Yoshida because if the bits are not prime, then the values of s bits which are taken out with a period shorter then the 2^n-1 bit period will be repeated, and the randomness will be impaired (Yoshida column 1, lines 45-55).

As to claim 2, the modified Iwamura discloses a method for generating pseudo-random numbers as defined in claim 1. The modified Iwamura fails to teach wherein the initial state value is processed by Hash function to determine its Hash value to adopt a prime number most approximated to the Hash value as the derived number.

However, Smeets discloses wherein the initial state value is processed by Hash function to determine its Hash value to adopt a prime number most approximated to the Hash value as the derived number (Smeets page 1, paragraph 0016 and page 7, paragraphs 0152-0156).

It would be obvious to one of ordinary skill in the art at the time of the applicant's invention to combine Iwamura and Smeets because a hash function makes it virtually impossible

to determine the input of the function on the basis of the output, which greatly increases the security of the generated random numbers/sequence (Smeets page 2, paragraph 0036).

As to claim 3, Iwamura discloses a method for generating pseudo-random numbers as defined in claim 1, wherein the reconstruction of the linear feedback shift resistor is carried out using Berlekamp-Massay algorithm (Iwamura column 2, lines 53-62).

As to claim 4, Iwamura discloses a method for generating pseudo-random numbers as defined in any of claims 1, which further comprises an eighth step for subjecting the pseudo-random numbers generated in the seventh step to nonlinear conversion (Iwamura column 10, lines 48-54).

As to claim 5, Iwamura discloses a pseudo-random number generator comprising:

a linear feedback shift register having n shift resistors and capable of outputting a bit string having bit number of (2 n)-1 per one cycle (Iwamura column 9, lines 19-55);

means for setting up an initial state value of the linear feedback shift register based on a secret key (Iwamura column 4, lines 16-30);

means for determining a derived value prime to the bit number per one cycle of the linear feedback shift register based on the initial state value by means of a predetermined operation processing (Iwamura column 2, lines 42-52);

means for outputting a bit string corresponding to the bit number calculated by the above means based on the initial state value from the linear feedback shift register (Iwamura column 3, lines 35-45);

means for taking out a bit from the output bit string every the number of the derived value to generate a new bit string (Iwamura column 9, lines 29-35);

means for reconstructing the linear feedback shift register such that the new bit string can be outputted from the resistor (Iwamura column 9, lines 40-45); and

means for generating pseudo-random numbers based on the initial state value from the reconstructed linear feedback shift register (Iwamura column 9, lines 19-55). Iwamura fails to teach means for multiplying the derived value by a value obtained by multiplying the bit number corresponding to one cycle by two or more to calculate a bit numbers to be outputted from the first linear feedback shift register.

However, Yoshida discloses means for multiplying the derived value by a value obtained by multiplying the bit number corresponding to one cycle by two or more to calculate a bit numbers to be outputted from the first linear feedback shift register (Yoshida column 1, lines 45-55).

It would be obvious to one of ordinary skill in the art at the time of the applicant's invention to combine Iwamura and Yoshida because multiplying the bit number by two or more increases the randomness of the generated random number (Yoshida column 1, lines 45-55).

As to claim 6, Iwamura discloses a pseudo-random number generator as defined in claim 5, which is further provided with means for generating a second linear feedback shift resistor having construction capable of outputting a new bit string, instead of the means for reconstructing the linear feedback shift resistor; and wherein the means for generating pseudo-random numbers generates the pseudo-random numbers based on the initial state value from the second linear feedback shift resistor (Iwamura column 12, lines 60-67 and column 13, lines 1-7).

As to claim 7, Iwamura discloses a pseudo-random number generator comprising:

a part for outputting a selectively used random number bit string having a predetermined bit number based on a secret key (Iwamura column 4, lines 15-30);

a part for outputting an amplified random number bit string having bits of a larger bit number than the selectively used random number bit string based on the selectively used random number bit string outputted from the part for outputting a selectively used random number bit string (Iwamura column 12, lines 40-44); and

a part for nonlinearly converting the amplified random number bit string outputted from the part for outputting an amplified random number bit string to output pseudo-random numbers (Iwamura column 10, lines 6-48);

said part for outputting a selectively used random number bit string comprising:

a linear feedback shift register having n shift resistors and capable of outputting a bit string having bit number of (2 n)-1 per one cycle (Iwamura column 9, lines 19-55),

means for setting up an initial state value of the linear feedback shift register based on a secret key (Iwamura column 4, lines 16-30),

means for determining a derived value prime to the bit number per one cycle of the linear feedback shift register based on the initial state value by means of a predetermined operation processing (Iwamura column 2, lines 42-52),

means for outputting a bit string corresponding to the bit number calculated by the above means based on the initial state value from the linear feedback shift register (Iwamura column 3, lines 35-45),

means for taking out a bit from the output bit string outputted from the above means every the number of the derived value to generate a new bit string (Iwamura column 9, lines 29-35),

means for reconstructing the linear feedback shift register such that the new bit string can be outputted from the resistor (Iwamura column 9, lines 40-45), and

means for outputting selectively used pseudo-random numbers based on the initial state value using the reconstructed linear feedback shift register reconstructed by the above means (Iwamura column 9, lines 19-55);

said part for outputting an amplified random number bit string comprising:

a random number table in which a plurality of amplified random bit strings having larger bit number than that of the selectively used random number bit string is stored (Iwamura column 12, lines 40-45), and

means capable of selecting a corresponding amplified random number bit string from the plurality of amplified random number bit strings within the random number table by referring to the random number table using the selectively used random number bit string outputted from the means for outputting selectively used random number bit string (Iwamura column 11, lines 15-20); and

said part for nonlinearly converting the amplified random number bit string comprising means for nonlinearly converting the amplified random number bit string selected by the means for selecting the amplified random number bit string by a nonlinear function to output pseudo-random numbers (Iwamura column 10, lines 6-48). Iwamura fails to teach means for multiplying

the derived value by a value obtained by multiplying the bit number corresponding to one cycle by two or more to calculate a bit numbers to be outputted from the linear feedback shift register.

However, Yoshida discloses means for multiplying the derived value by a value obtained by multiplying the bit number corresponding to one cycle by two or more to calculate a bit numbers to be outputted from the first linear feedback shift register (Yoshida column 1, lines 45-55).

It would be obvious to one of ordinary skill in the art at the time of the applicant's invention to combine Iwamura and Yoshida because multiplying the bit number by two or more increases the randomness of the generated random number (Yoshida column 1, lines 45-55).

As to claim 8, Iwamura discloses a pseudo-random number generator as defined in claim 7, wherein said part for outputting an amplified random number bit string comprises means for generating the amplified random number bit string by a secret key given, and means for storing the amplified random bit string generated from the above means in the random number table, and carrying out initial setup of the random number table (Iwamura column 10, lines 15-19).

As to claim 9, Iwamura discloses a pseudo-random number generator as defined in claim 7, wherein:

the means for outputting selectively used random number table are plurally provided in said part for outputting a selectively used random number bit string (Iwamura column 4, lines 15-30),

the random number table is provided to correspond to each of the means for outputting selectively used random number table in said part for outputting an amplified random number bit string (Iwamura column 12, lines 40-44),

the means for generating the amplified random number bit string selects a corresponding amplified random number bit string from the random number table by referring to the random number table corresponding to each of the means for outputting selectively used random number bit string respectively using the selectively used random number bit strings outputted from each of the means for outputting selectively used random number bit string (Iwamura column 12, lines 40-44), and

the means for nonlinearly converting outputs pseudo-random numbers by nonlinearly converting the amplified random number bit string selected from each of the random number tables by nonlinear function using each of the means for generating the amplified random bit string in said part for nonlinearly converting the amplified random number bit string (Iwamura column 10, lines 6-48).

As to claim 10, Iwamura discloses a pseudo-random number generator as defined in claim 9, wherein plural random number tables are provided corresponding to each of the means for outputting selectively used random number bit string in said part for outputting an amplified random number bit string, and which is further provided with means for subjecting each of the amplified random number bit strings selected from each of the random number tables by the means for selecting the amplified random number bit string to exclusive-or operation every the means for outputting a selectively used random number bit string of the part for outputting a selectively used random number bit string and outputting to the nonlinear conversion means (Iwamura column 11, lines 15-20).

As to claim 11, Iwamura discloses a pseudo-random number generator as defined in claim 9, wherein said part for outputting an amplified random number bit string is further

provided with means for replacing the random number tables with each other at a predetermined time (Iwamura column 3, lines 35-45).

As to claim 12, Iwamura discloses a pseudo-random number generator as defined in claim 11, wherein the means for replacing the random number tables in said part for outputting a selectively used random number bit string has function of replacing the random number tables with each other every time that the means for outputting a selectively used random number bit string outputs the selectively used random number bit string required for referring to each of the random number tables (Iwamura column 5, lines 17-29).

As to claim 13, Iwamura discloses a pseudo-random number generator as defined in claim 11, wherein the means for replacing the random number tables has function of generating random number for replacing random number tables having the same number as that of each of the random numbers, giving the random numbers for replacing random number tables to each of the random number tables as a table number of random number table, and replacing order of the random number (Iwamura column 5, lines 17-29).

As to claim 14, Iwamura discloses a program to be executed by a computer for generating pseudo-random numbers comprising:

a part for outputting a selectively used random number bit string having a predetermined bit number based on a secret key (Iwamura column 4, lines 15-30);

a part for outputting an amplified random number bit string having bits of a larger bit number than the selectively used random number bit string based on the selectively used random number bit string outputted from the part for outputting a selectively used random number bit string (Iwamura column 12, lines 40-44); and

a part for nonlinearly converting the amplified random number bit string outputted from the part for outputting an amplified random number bit string to output pseudo-random numbers (Iwamura column 10, lines 6-48);

said part for outputting a selectively used random number bit string comprising:

a linear feedback shift register having n shift resistors and capable of outputting a bit string having bit number of (2 n)-1 per one cycle (Iwamura column 9, lines 19-55),

means for setting up an initial state value of the linear feedback shift register based on a secret key (Iwamura column 4, lines 16-30),

means for determining a derived value prime to the bit number per one cycle of the linear feedback shift register based on the initial state value by means of a predetermined operation processing (Iwamura column 2, lines 42-52),

means for outputting a bit string corresponding to the bit number calculated by the above means based on the initial state value from the linear feedback shift register (Iwamura column 3, lines 35-45),

means for taking out a bit from the output bit string outputted from the above means every the number of the derived value to generate a new bit string (Iwamura column 9, lines 29-35),

means reconstructing of the linear feedback shift register such that the new bit string can be outputted from the resistor (Iwamura column 9, lines 40-45), and

means for outputting selectively used pseudo-random numbers based on the initial state value using the reconstructed linear feedback shift register reconstructed by the above means (Iwamura column 9, lines 19-55),

said part for outputting an amplified random number bit string comprising:

a random number table in which a plurality of amplified random bit strings having larger bit number than that of the selectively used random number bit string is stored (Iwamura column 12, lines 40-45), and

means capable of selecting a corresponding amplified random number bit string from the plurality of amplified random number bit strings within the random number table by referring to the random number table using the selectively used random number bit string outputted from the means for outputting selectively used random number bit string (Iwamura column 11, lines 15-20); and

said part for nonlinearly conversing the amplified random number bit string comprising means for nonlinearly conversing the amplified random number bit string selected by the means for selecting the amplified random number bit string by a nonlinear function to output pseudo-random numbers (Iwamura column 10, lines 6-48). Iwamura fails to teach means for multiplying the derived value by a value obtained by multiplying the bit number corresponding to one cycle by two or more to calculate a bit numbers to be outputted from the linear feedback shift register.

However, Yoshida discloses means for multiplying the derived value by a value obtained by multiplying the bit number corresponding to one cycle by two or more to calculate a bit numbers to be outputted from the first linear feedback shift register (Yoshida column 1, lines 45-55).

It would be obvious to one of ordinary skill in the art at the time of the applicant's invention to combine Iwamura and Yoshida because multiplying the bit number by two or more increases the randomness of the generated random number (Yoshida column 1, lines 45-55).

As to claim 15, Iwamura discloses a program to be executed by a computer as defined in claim 14, further comprising means for generating the amplified random number bit string by a given secret key, storing the bit string in a random number table, and carrying out initial setup of the random number table, in the part for outputting an amplified random number bit string (Iwamura column 10, lines 15-19).

As to claim 16, Iwamura discloses a program to be executed by a computer as defined in claim 14 ~~15~~, wherein:

the means for outputting selectively used random number table are plurally provided in said part for outputting a selectively used random number bit string (Iwamura column 4, lines 15-30),

the random number table is provided to correspond to each of the means for outputting selectively used random number table in said part for outputting an amplified random number bit string (Iwamura column 12, lines 40-44),

the means for generating the amplified random number bit string selects a corresponding amplified random number bit string from each of the random number tables by referring to the random number table corresponding to every each of the means for outputting selectively used random number bit string using the selectively used random number table outputted from each of the means for outputting selectively used random number bit string (Iwamura column 12, lines 40-44), and

the means for nonlinearly converting outputs pseudo-random numbers by nonlinearly converting the amplified random number bit string selected from each of the random number tables using each of the means for generating the amplified random number bit strings in said

part for nonlinearly converting the amplified random number bit string (Iwamura column 10, lines 6-48).

As to claim 17, Iwamura discloses a program to be executed by a computer as defined in claim 16, wherein plural random number tables are provided every each of the means for outputting selectively used random number bit string in said part for outputting an amplified random number bit string and which is further provided with means for subjecting each of the amplified random number bit strings selected from each of the random number tables by the means for selecting the amplified random bit string to exclusive-or operation every the means for outputting selectively used random number bit string of said part for outputting a selectively used random number bit string and ~~and~~ outputting to the means for nonlinearly conversing of said part for nonlinearly conversing the amplified random number bit string (Iwamura column 11, lines 15-20).

As to claim 18, Iwamura discloses a program to be executed by a computer as defined in claim 17, which is further provided with means for replacing the random number tables with each other at a predetermined time in said part for outputting an amplified random number bit string (Iwamura column 11, lines 15-20).

As to claim 19, Iwamura discloses a program to be executed by a computer as defined in claim 18, wherein the means for replacing the random number tables has function of replacing the random number tables with each other every time that the means for outputting the selectively used random number bit strings of the part for outputting a selectively used random number bit string outputs the selectively used random number bit string required for referring to each of the random number tables (Iwamura column 3, lines 35-45).

As to claim 20, Iwamura discloses a program to be executed by a computer as defined in claim 18, wherein the means for replacing the random number tables has function of generating random numbers for replacing random number tables having the same number as that of each of the random numbers, giving the random numbers for replacing random number tables to each of the random number tables as a table number of random number table, and replacing order of the random number tables according to a rule predetermined based on the table number (Iwamura column 5, lines 17-29).

Prior Art

13. US 20050010624 is pertinent because it teaches… The invention pertains to a method for making secure a generator generating pseudo-random numbers. The generator is characterized by its internal status. The generator includes: a first storage zone containing status bits, representing the internal status of the generator; a computing unit performing arithmetic operations on the status bits to produce the pseudo-random numbers and to modify the status bits; a second storage zone containing the pseudo-random numbers; a single output for reading the pseudo-random numbers contained in the second storage zone. The method according to the invention includes the step of irreversibly and unconditionally inhibiting, in particular via logical and/or mechanical and/or electronic means, the reading and the writing of the status bits from outside the generator, including via the single output. US 5566099 is pertinent because it teaches… A pseudorandom number generator which uses linear feedback shift registers and a nonlinear function circuit and can make the conditioned output distribution of generated pseudorandom numbers uniform even if the conditioned output distribution of the nonlinear function circuit has some deviation. The generator has a shift register to which the output of the nonlinear function circuit is inputted as a

serial input, an initial value setting circuit for setting random initial values to the linear feedback shift registers and the shift registers, and an adder for adding predetermined bits of the parallel outputs of the register and outputting a pseudorandom number stream. The generator can be used to generate a cryptogram which cannot be deciphered by the correlation attack method.
US 5910907 is pertinent because it teaches… An apparatus for, and method of, generating a k-bit pseudorandom number using m storage devices, m being less than k, is provided. The apparatus has interconnections among the storage devices. The interconnections include modulo-2 adders, and preferably 2-input modulo-2 adders, providing feedback to the storage devices. Some adders have outputs coupled to inputs of the storage devices while others have outputs coupled to k output lines. The interconnections are derived according to an m'th order generating polynomial and arranged to implement the generating function thereby outputting k bits on the k output lines each cycle of a clock signal common to the storage devices.

Conclusion

14. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Rebecca L. Pachura whose telephone number is (571) 270-3402. The examiner can normally be reached on Monday-Thursday 7:30 am-6:00 pm est.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami can be reached on (571) 272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Rebecca L Pachura/
Examiner, Art Unit 2136

/Nasser G Moazzami/
Supervisory Patent Examiner, Art Unit 2136